3DAssurance
Delivering Security Risk Assurance

Why Dave doesn't talk to Steve* and other Findings

*other names and genders are available

1

3DAssurance
Delivering Security Risk Assurance

A tale of two silos

- Acts of unlawful interference with civil aviation
  - Traditionally physical, increasingly cyber, and now hybrid
- Different focus but many crossovers
  - Physical – Counter Terrorism/prevent unlawful interference
  - Cyber – acquisitional crime, hacking, data protection, business disruption, protect systems
- Different reporting lines, models, language, separate risk registers, risk management techniques
- Limited collaboration, some communication

2

2

3DAssurance
Delivering Security Risk Assurance

Hybrid Risks: we keep telling our clients its not just about physical security

- Alleged plot to blow up Amazon Data Centres (US)
- Bitcoin bomb threats doing the rounds again
- Disabling CCTV over IP Networking
- Penetration of Building Management Systems
- Creative targeting of aviation (offsetting navigation aids)
- Disabling Critical National Infrastructure
- USB sticks loss/theft
- Insider cyber attacks are often easier than Insider physical attacks, and harder to detect. This is true of external attacks too
- More activity by hostile states

3

3

3DAssurance
Delivering Security Risk Assurance

Identifying *warning signals has become more complex for the aviation sector*

- Identification of 'warning signals' is key
- The sector has suffered from missed warning signals
- Hybrid threats increase the risk of warning signals being missed
- Perceived/mis-assessed/wrong assumptions/ threat
- Industry watch – why we need to learn from others
- "Too difficult" box – regular monitoring as a minimum
- A SeMS approach with its relentless focus on threat and risk will help improve aviation 'risk radars'

4

4

3DAssurance
Delivering Security Risk Assurance

A dog is not just for Christmas, and security culture is not just for 2021

- ICAO 2021 - Year of Security culture – good to focus on culture, but not just for this year
- Security culture has to be part of the organisations DNA
- A project or course alone will not grow a positive security culture
- Growing positive security cultures is difficult and take time
- As the SeMS Framework* points out, Management commitment and leaders *walking the talk* are key

*CAP1223 Framework for an Aviation Security Management System

5

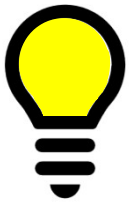
5

3DAssurance
Delivering Security Risk Assurance

Some good news: SeMS is easy
Joining up, collaborating, fine-tuning...not something new

Initial worries about implementing SeMS

- More work
- Just another management fad
- Potential wasted effort
- Duplication
- Distraction from the day job
- Diversion of scarce resources



"We soon realised that our worries were unfounded and the effort we invested in the early stages of implementation made our security management and the whole day job easier"

6

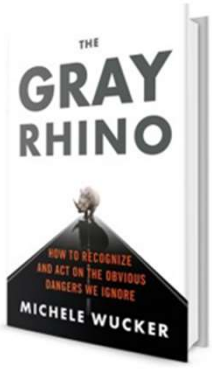
6

3DAssurance
Delivering Security Risk Assurance

Tackling AvSec's Gray Rhino with SeMS

The Gray Rhino: an obvious danger we ignore

- 9/11, the 2008 financial crash, the COVID-19 crisis, etc
- Not random surprises: precedents, warning signals, visible evidence



- The hybrid attack is a Gray Rhino charging towards us
- Succession of "InfoSec" attacks illustrating our vulnerability
- Cyber security has been on many AvSec "watchlists" for years
- We cannot afford to ignore the warning signals

7

7

3DAssurance
Delivering Security Risk Assurance

How SeMS is tackling the Gray Rhino

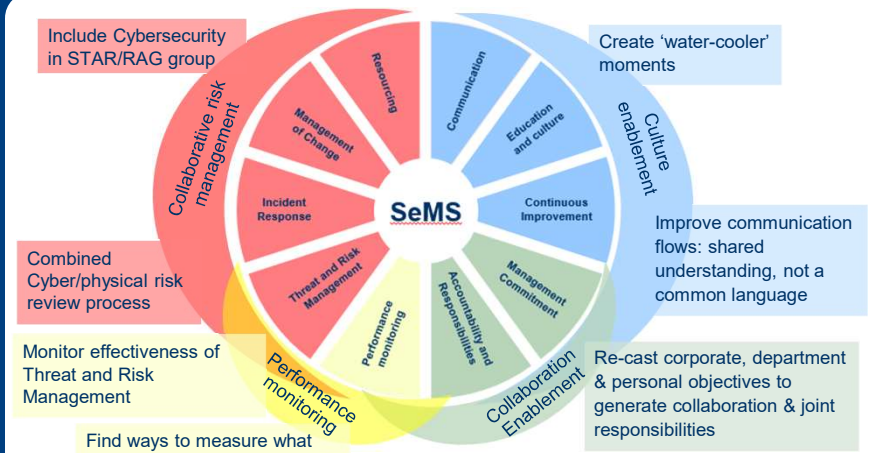
CAP1223	SeMS Components	Development of collaboration
Culture & Collaboration enablement	Communication	Explain disparate terminology and techniques
	Education and culture	Explain disparate terminology and techniques
	Continuous improvement	Co-operate on improving "as done" vs "as imagined"
	Management commitment	Security strategy for collaboration cascading to corporate and department objectives
	Accountability and responsibilities	Accountabilities and personal objectives cascade from objectives
Collaborative risk management	Performance Monitoring	Learn where collaboration is/is not working, or objectives are/are not achieveable
	Threat and risk management	Relentless focus: collaboration at upper levels, details in silos; common principles, disparate techniques
	Incident response	Share incident histories and lessons; collaborate in response to hybrid incidents
	Management of change	Share change plans; identify cross-impacts; collaborate on hybrid changes
	Resourcing	Resourcing follows objectives to ensure collaboration is resourced

8

8

3DAssurance
Delivering Security Risk Assurance

Key lessons and suggestions



9

9

3DAssurance
Delivering Security Risk Assurance

An Inspector calls: the proof of the pudding!

"and he didn't even want to see my SeMS Manual!"

10

10